Inconsistency of the Zermelo-Fraenkel set theory with the axiom of choice and its effects on the computational complexity

Minseong Kim
Hankuk Academy of Foreign Studies

2012/02/21

1 Introduction

This paper exposes a contradiction in the Zermelo-Fraenkel set theory with the axiom of choice (ZFC). While Gödel's incompleteness theorems state that a consistent system cannot prove its consistency, they do not eliminate proofs using a stronger system or methods that are outside the scope of the system. The paper shows that the cardinalities of infinite sets are uncontrollable and contradictory. The paper then states that Peano arithmetic, or first-order arithmetic, is inconsistent if all of the axioms and axiom schema assumed in the ZFC system are taken as being true, showing that ZFC is inconsistent. The paper then exposes some consequences that are in the scope of the computational complexity theory.

2 Hilbert's first and second problem

2.1 First problem: continuum hypothesis

Definition 2.1. The power set of a set X is defined as the set of all subsets of X.

Definition 2.2. A set has the cardinality of $\aleph_0$ if the set can form a direct bijection with the set of all natural numbers, $\mathbb{N}$.

Definition 2.3. A countable set is a set with the cardinality of $\aleph_0$. An uncountable set is a set that has the cardinality bigger than $\aleph_0$.

Definition 2.4. $\aleph_{k+1}$ is the successor cardinal of $\aleph_k$ where $k \in \mathbb{N}$. There is no cardinal number between $\aleph_k$ and $\aleph_{k+1}$.

Theorem 2.1. Cantor's Theorem. *The cardinality of the power set of a set X is bigger than the cardinality of the set X. Suppose that a set X has the cardinality of $\aleph_k$ where $k \in \mathbb{N}$. Then, the cardinality of the power set of the set X is $2^{\aleph_k}$. Representing the power set of the set X as the set $\mathcal{P}(X)$, $X \subsetneq \mathcal{P}(X)$ as $|X| < |\mathcal{P}(X)|$. [5] The results of Cantor's diagonal argument shows that the set of the cardinality $2^{\aleph_k}$ is not in bijection with the set of the cardinality $\aleph_k$.*

Conjecture 2.2. Continuum Hypothesis. *Set Y where $\aleph_0 < |Y| < 2^{\aleph_0}$ does not exist.*

Corollary 2.3. *As $\aleph_1$ is the successor cardinal of $\aleph_0$, if continuum hypothesis holds, $2^{\aleph_0} = \aleph_1$.*

Statement 2.4. *The works of Kurt Gödel prove that continuum hypothesis (CH) and the axiom of choice are consistent with ZF.[4] The works of Paul Cohen prove that the negation of CH is also consistent with ZFC. [2, 3, 6]*

Conjecture 2.5. Generalized Continuum Hypothesis. *Set Y where $\aleph_k < |Y| < 2^{\aleph_{k+1}}$ does not exist.*

Corollary 2.6. *As $\aleph_{k+1}$ is the successor cardinal of $\aleph_k$ where $k \in \mathbb{N}$, if generalized continuum hypothesis (GCH) holds, $2^{\aleph_k} = \aleph_{k+1}$.*

Statement 2.7. *The works of Wacaw Sierpiński show that $ZF + GCH$ implies the axiom of choice (AC).*

2.2 Gödel's incompleteness theorems

Theorem 2.8. first theorem. *No consistent formal system is capable of expressing the theory of natural numbers completely. Any formal system that claims to express the theory of natural numbers is incomplete; therefore, such system will have a true statement in the language that is unprovable. [8]*

Theorem 2.9. second theorem. *Any consistent formal system capable of containing truth of basic arithmetic and formal provability cannot prove its own consistency. [8]*

Corollary 2.10. *A consistency proof of any consistent formal system can only be done using a stronger system.*

2.3 Gentzen's consistency proof

Definition 2.5. $\varepsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\}$ where ω is the smallest transfinite ordinal and sup represents supremum. ε_0 is countable.

Theorem 2.11. Gentzen's consistency proof. *Over the base theory of primitive recursive arithmetic (PRA), the quantifier free transfinite induction of Peano arithmetic holds up to ε_0. [7]*

Conjecture 2.12. *It has been conjectured that the quantifier free transfinite induction over the base theory of PRA up to ε_0 is enough to show that Peano arithmetic is consistent.*

Statement 2.13. *Hilbert's second problem is interpreted as asking whether Peano arithmetic is consistent.*

Statement 2.14. *It has not been clear whether Gentzen's consistency proof and Gödel's incompleteness theorems resolve the Hilbert's second problem.*

Statement 2.15. *In the latter part of this paper, we will disprove Conjecture 2.12.*

3 Inconsistency of the ZFC system

Definition 3.1. The cardinality of the set of all finite strings (S), $|S| = \aleph_0$ as done conventionally. All strings are assumed finite.

Definition 3.2. The cardinality of the set of all base problems (P) are assumed $|P| = 2^{\aleph_0}$, as done conventionally.

Definition 3.3. Let us define a set, E. Every set that has $\aleph_0$ base problems from the set P as its elements is an element of the set E.

Statement 3.1. *It is evident that $|P| = |E|$, as $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$.*

Statement 3.2. *The axiom of choice and the well-ordering theorem are equivalent. This implies that even an uncountable set can be well-ordered by a strict total order.*

Statement 3.3. *It is possible to construct a system where each base problem is represented by a single-spaced picture, not by a countable group of strings. Compressing a group of strings into a single-spaced picture and adding random dots, or compressing and assigning an ordinal number to each base problem can be done to construct a such system, as allowed by the axiom of choice.*

Statement 3.4. *It is possible to construct a system where each base problem has a single and unique representation.*

Definition 3.4. It is possible to construct a system that has the characteristics of the two systems aforementioned. Let us define a such system as SYS.

Definition 3.5. Let us define a set U. The set consists of some specific $\aleph_0$ elements from the set P and the $\aleph_0$ elements that do not have any meaning assigned. The subset of U that contains the $\aleph_0$ elements that do not have any meaning assigned is defined as the set H.

Definition 3.6. Let us define a set, V. Every set that has $\aleph_0$ problems from the set U as its elements is an element of the set V. Let us also define a set, J. Every set that has $\aleph_0$ problems (elements) from the set H as its elements is an element of the set J.

Statement 3.5. *As* ${\aleph_0}^{\aleph_0}$ *equals to* $2^{\aleph_0}$, $|V| = |E|$.

Theorem 3.6. *There are some cases possible in ZFC that contradict Cantor's theorem and diagonal argument.*

Proof.

Statement 3.7. *Let us represent the sets* E *and* V *using* SYS. *As* $|E| = |V|$, *There must be a bijection from the set* E *to* V *or vice versa.*

Statement 3.8. *Eliminating the elements that are both in the sets* E *and* V, *we are left with the elements of the subset* J *in the set* V *and the remaining* $2^{\aleph_0}$ *elements in the set* E.

Statement 3.9. *There must be a bijection from the subset* J *of the set* V *to the set of the remaining elements of the set* E, *now defined as the set* T. *We define the set of the elements in the single space of the elements, or the remaining base problems, of* T *as* O. $|O| = 2^{\aleph_0}$, *as* $2^{\aleph_0} - \aleph_0 = 2^{\aleph_0}$.

Recall Statement 3.3 and 3.4. As SYS follows the statement, each problem cannot be assigned more than one representation, and the representation has to be single-spaced. Therefore,

Lemma 3.10. *The elements of the set* H *occupies each space of the elements of* $\aleph_0$*-spaced elements of the set* J. *Similarly, the elements of the set* O *occupies each space of the elements of the set* T. *As we represent each base problem and its combinations under the system* SYS, *and a base problem is set not to be broken down into several spaces, there must be a bijection from the set* H *that is a part of the set* J *to the set* O *that is a part of the set* T. *Therefore, there must be a bijection from a set that has the cardinality of* $2^{\aleph_0}$ *to a set that has the cardinality of* $\aleph_0$.

Statement 3.11. *Cantor's diagonal argument and consequent Cantor's theorem, as seen in Theorem 2.1, established that a set of the cardinality* $\aleph_0$ *cannot be placed in bijection with a set of the cardinality* $2^{\aleph_0}$. *Therefore, Lemma 3.10 contradicts Cantor's diagonal argument. Contradiction.*

In order to avoid this contradiction, we define the cardinality of the set of base problems, $|P|$ as $\aleph_0$. $|E| = 2^{\aleph_0}$, as ${\aleph_0}^{\aleph_0} = 2^{\aleph_0}$. Now, let us dig into Peano arithmetic.

Statement 3.12. *Operation of Peano arithmetic is on natural numbers. Each addition/subtraction/multiplication/division case can be represented by a tuple* $(x_1, x_2, \ldots, x_n)$. *Each* x_k *where* $k \in \mathbb{N}$ *represents a natural number that is added, subtracted, divided or multiplied by other numbers in the tuple using arithmetic procedure. If Peano arithmetic is consistent, it should not produce an error when doing operations on* $\aleph_0$ *natural numbers.*

Statement 3.13. *The set of all possible tuples of Peano arithmetic can be regarded as the power set of the set of natural numbers, when calculating the cardinality of all sets of them. Tuples also represent each arithmetic operation and problem. The cardinality of arithmetic problems is then* $2^{\aleph_0}$. *We represent the set of all possible tuples as* $\mathcal{P}(\mathbb{N})$.

As a result, contradiction:

Lemma 3.14. Contradiction. $\mathcal{P}(\mathbb{N}) \subsetneq P$. *However,* $|\mathcal{P}(\mathbb{N})| > |P|$. *Contradiction.*

The theorem is proven. □

Let us recall Conjecture 2.2, continuum hypothesis.

Theorem 3.15. *As ZFC is inconsistent in the cardinalities of infinite sets, continuum hypothesis is invalid in ZFC and there cannot be any meaningful comparison between two different transfinite cardinals.*

Statement 3.16. *The works of Kurt Gödel and Paul Cohen do not contradict the above results. While these works state that continuum hypothesis and the negation of it are consistent with ZFC, the assumption is that ZFC is consistent. When ZFC is inconsistent, the results of these works cannot be applied directly.*

Therefore,

Lemma 3.17. *Conjecture 2.12 is disproved.*

3.1 Consequence

From the above results, it is definite that ZFC is inconsistent. However, it is not really clear what causes this consistency. It is not clear whether inconsistency of Peano arithmetic causes inconsistency of ZFC, or inconsistency of axioms in ZFC leads to inconsistency of Peano arithmetic. There are several candidates to the source of inconsistency.

3.1.1 Axiom of choice

If we assume that the axiom of choice is inconsistent, it is impossible to pick a number or a set from a set that has infinite elements and assign some representation to it. This may solve the contradiction. In addition, as presented in Statement 2.7, ZF+GCH becomes inconsistent if the axiom of choice is shown inconsistent.

3.1.2 Single-spaced representation of a set and a number

If we assume that we cannot compress a symbol or a representation that represents a number or a set into a single place - this means that every problem has to be cast in form of a group of strings - the contradiction may be resolved.

3.1.3 Consistency proof of transfinite induction

Gentzen's consistency proof, Theorem 2.11, only provided consistency proof of quantifier-free transfinite induction over the base theory of PRA up to ε_0. Inconsistency may lie in the scope beyond ε_0.

3.1.4 Axioms and axiom schema of the ZF system

The axioms of the ZFC system may be the source of inconsistency. There can be a possibility that the axiom of extensionality, $\forall A \forall B \, (\forall C \, (C \in A \iff C \in B) \Rightarrow A = B$, the concept of a power set, or the axiom of infinity $(\exists \mathbf{I} \, (\emptyset \in \mathbf{I} \wedge \forall x \in \mathbf{I} \, (\, (x \cup \{x\}) \in \mathbf{I})))$ is the source of the contradiction. Modifying the axiom schema of restricted comprehension may resolve this inconsistency, but whether it really does is out of the scope of this paper.

4 Computaional Complexity Theory

The results aforementioned can be used to verify several known results in the computational complexity theory.

Statement 4.1. *Let us create an infinite-state non-deterministic Turing machine. [1] [9] We all know that an infinite-state (or $\aleph_0$-state) non-deterministic Turing machine is different from a finite-state non-deterministic Turing machine in sense that an infinite-state non-deterministic Turing machine is more powerful than a finite-state non-deterministic Turing machine and that an infinite-state non-deterministic Turing machine requires less time resource, usually represented by Big-O notation, to solve a certain problem. The fact that a finite-state non-deterministic Turing machine cannot simulate an infinite-state Turing machine with the exact performance speed can be proven using the results mentioned above.*

Proof. Let us present a $\aleph_0$-node graph. Assume that inter-node relationship of every node can be represented by a finite input string. Let us then say that both a finite-state non-deterministic Turing machine and an infinite-state non-deterministic Turing machine are in the state where no search of the graph occurred. A finite-state non-deterministic Turing machine can only choose a finite group of nodes to search at once. Therefore, the number of search options available for a single transition occurrence to a group of states to the machine is $\aleph_0$. These options will form the elements of a set AB. An infinite-state non-deterministic Turing machine has $2^{\aleph_0}$ search options available for a single transition occurrence. These options will form the elements of a set BC. If these two machines possess an equal power, we can set a rule and perform a surjection from the set BC to the set AB. However, as stated in Theorem 3.15, we cannot have any meaningful function between two sets that are of different transfinite cardinalities. As such, we cannot perform a surjection from the set BC to AB. Therefore, the power of a finite-state non-deterministic Turing

machine is different from the power of an infinite-state non-deterministic Turing machine. □

4.0.5 Savitch's Theorem and a contradiction

Let us again present a $\aleph_0$-node graph. Assume that inter-node relationship of every node can be represented by a finite string. Let us then say that both a finite-state non-deterministic Turing machine and a finite-state deterministic Turing machine are in the state where no search of the graph occurred. Let us create $\aleph_0$ deterministic Turing machines and $\aleph_0$ non-deterministic Turing machines. Each machine is given a specific node different from others that it has to search. We then create the group of deterministic machines and the group of non-deterministic machines. Except node choices, every machine in each group is equivalent. Let us state the following:

Statement 4.2. *The complexity class NP can be represented by $NP = \bigcup_{c\in\mathbb{N}} NTIME(n^c)$. Similarly, the complexity class P can be represented by $P = \bigcup_{c\in\mathbb{N}} DTIME(n^c)$. [1]*

Let us look at the number of cases possible in each group when starting the machines at the same time. As each deterministic Turing machine can only choose one node to search, it can only search the node it must travel at once. Therefore, there is only one possible combination of the group each time, or at $O(1)$. However, there are ${\aleph_0}^k = \aleph_0$ actions possible for each non-deterministic Turing machine, where $k \in \mathbb{N}$ and k is some defined number of states. Therefore, the total number of the possible combinations of the group of non-deterministic Turing machines is ${\aleph_0}^{\aleph_0} = 2^{\aleph_0}$. Let us create a set of possible combinations of the group of deterministic Turing machines as the set SP and that of the group of non-deterministic Turing machines as the set SNP. We then look at the length of the finite input. Let us run every machine $O(n^c)$ times, where n is the length of the finite input and c is some specified constant. When running, add every possible combination into the set that a machine is in each time. When the machines stop running, $|SP| = 1 * n^c = n^c$, $|SNP| = 2^{\aleph_0} * n^c = 2^{\aleph_0}$. If $P = NP$, we can set a rule and perform a surjection from the set SNP to SP. Recall Theorem 3.15, which states that there cannot be any meaningful functional relationship between the two sets that have different cardinalities of transfinite cardinal numbers. As such, we cannot perform a surjection between the two sets. Therefore,

Lemma 4.3. *all of the aforementioned consequences imply that $P \neq NP$.*

However, this should also apply to the case of the complexity of space bounds, such as $PSPACE$ and $NPSPACE$.

Statement 4.4. Savitch's Theorem: *$NSPACE(f(n)) \subseteq DSPACE\left((f(n))^2\right)$; therefore, as $PSPACE = \bigcup_{k\in\mathbb{N}} DSPACE(n^k)$ and $NPSPACE = \bigcup_{k\in\mathbb{N}} NSPACE(n^k)$, it is evident that $PSPACE = NPSPACE$.*

Statement 4.5. *However, the results above show that $PSPACE \neq NPSPACE$. Therefore, a contradiction occurs.*

The result at first seems implausible. However, when ZFC is inconsistent, any possible contradiction that concurs with inconsistency can occur. At this point, one may reason that as $PSPACE = NPSPACE$, to be consistent with the contradiction, $P \neq NP$. However, at this point, it seems unclear whether this type of reasoning can be used to assert the claim.

5 Conclusion

This paper shows inconsistency of the ZFC system, and states that continuum hypothesis itself is invalid, as we cannot compare two sets that have different transfinite cardinalities. The paper then presents how the computational complexity theory is affected when there is inconsistency of the ZFC system. Following from the consequences, the paper provides alternative proofs of the theorems, and exposes a contradiction in the computational complexity theory interpreted in the ZFC system.

References

[1] S. Arora and B. Barak, *Nondeterministic Turing machines*, Computational Complexity, 41–42.

[2] P. Cohen, *The Independence of the Continuum Hypothesis, II*, 1964, Proceedings of the National Academy of Sciences of the United States of America 51 (1): 105110.

[3] P. Cohen, *The Independence of the Continuum Hypothesis, I*, 1963, Proceedings of the National Academy of Sciences of the United States of America 50 (6): 11431148.

[4] K. Gödel, *The Consistency of the Continuum-Hypothesis*, Princeton University Press, 1940.

[5] Y. Lin, L. Levin, and M. Luby, *Set Theory: An Intuitive Approach*, Houghton Mifflin Harcourt (1974) pp. 108-109.

[6] Y. Lin, L. Levin, and M. Luby, *Set Theory: An Intuitive Approach*, Houghton Mifflin Harcourt (1974) pp. 124-125.

[7] G. Gentzen, *Die Widerspruchfreiheit der reinen Zahlentheorie*, Mathematische Annalen (1936), 112:493565

[8] M. Hirzel, *On formally undecidable propositions of Principia Mathematica and related systems I*, http://www.research.ibm.com/people/h/hirzel/papers/canon00-goedel.pdf

[9] T. Ord, *Hypercomputation: computing more than the Turing machine*, http://arxiv.org/ftp/math/papers/0209/0209332.pdf